

IMAGE DATA CIPHERING METHOD

Patent Number: JP6125553

Publication date: 1994-05-06

Inventor(s): NAKAI TOSHIHISA

Applicant(s): OKI ELECTRIC IND CO LTD

Requested Patent: ☐ JP6125553

Application

Number: JP19920273138 19921012

Priority Number

(s):

IPC Classification: H04N7/167; G06F15/66; G09C5/00; H04L9/06; H04L9/14; H04N1/41; H04N1/415; H04N1/44; H04N7/133

EC Classification:

Equivalents:

Abstract

PURPOSE: To reduce the processing amount for ciphering.

CONSTITUTION: Inputted image signals are divided into blocks by a blocking part 102, a DCT conversion is performed for the divided blocks by a DCT part 103, and DC components $f(0, 0)$ and AC components $f(i, j)$ are outputted. The DC components $f(0, 0)$ are quantized by a DC quantizing part 104, are ciphered a ciphering part 110 and are delivered to a multiplexing part 131. The AC components $f(i, j)$ is quantized by an AC quantizing part 105 and is delivered to the multiplexing part 131 after an entropy encoding is performed for the components by an AC entropy encoding part 120. In the multiplexing part 131, the output of the ciphering part 110 and the output of the AC entropy encoding part 120 is multiplexed and outputted. Thus, the only DC components of image data are ciphered.

Data supplied from the **esp@cenet** database - 12

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-125553

(43)公開日 平成6年(1994)5月6日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 N 7/167		8943-5C		
G 0 6 F 15/66	3 3 0 H	8420-5L		
G 0 9 C 5/00		8837-5L		
H 0 4 L 9/06		7117-5K	H 0 4 L 9/ 02	Z

審査請求 未請求 請求項の数 3(全 17 頁) 最終頁に続く

(21)出願番号 特願平4-273138

(22)出願日 平成4年(1992)10月12日

(71)出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72)発明者 中井 敏久

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

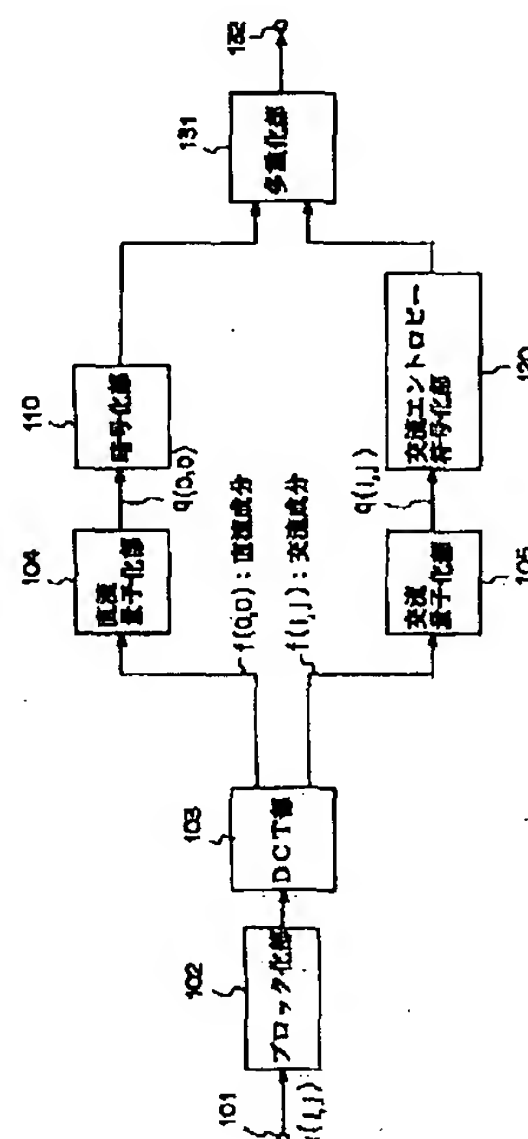
(74)代理人 弁理士 柿本 恭成

(54)【発明の名称】 画像データ暗号化方法

(57)【要約】

【目的】 暗号化のための処理量を少なくする。

【構成】 入力された画像信号がブロック化部102でブロックに分割され、その分割されたブロックがDCT部103でDCT変換され、直流成分 $f(0,0)$ と交流成分 $f(i,j)$ が出力される。直流成分 $f(0,0)$ は、直流量子化部104で量子化され、暗号化部110で暗号化されて多重化部131へ送られる。交流成分 $f(i,j)$ は、交流量子化部105で量子化され、交流エントロピー符号化部120でエントロピー符号化された後、多重化部131へ送られる。多重化部131では、暗号化部110の出力及び交流エントロピー符号化部120の出力を多重化して出力する。これにより、画像データのうちの直流成分だけが暗号化される。



本発明の第1の実施例の画像データ暗号化方法

【特許請求の範囲】

【請求項1】 圧縮した画像データを暗号化する画像データ暗号化方法において、

2次元の画像信号を n 画素 \times n 画素のブロックに分割する分割処理と、

前記分割処理で分割されたブロックを離散コサイン変換する離散コサイン変換処理と、

前記離散コサイン変換処理の出力のうちの直流成分を量子化する直流量子化処理と、

前記離散コサイン変換処理の出力のうちの交流成分を量子化する交流量子化処理と、

前記直流量子化処理の出力を暗号化する暗号化処理と、

前記交流量子化処理の出力をエントロピー符号化する交流エントロピー符号化処理と、

前記暗号化処理の出力と前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、

実行することを特徴とする画像データ暗号化方法。

【請求項2】 前記直流量子化処理では、出力信号を n ビットの固定長符号に符号化する固定長符号化処理を行い、

前記暗号化処理では、前記直流量子化処理の出力に対して n ビット毎に暗号化し、

前記多重化処理では、1ブロック毎に前記暗号化処理の出力と前記交流エントロピー符号化処理の出力を多重化することを特徴とする請求項1記載の画像データ暗号化方法。

【請求項3】 圧縮した画像データを暗号化する画像データ暗号化方法において、

2次元の画像信号を n 画素 \times n 画素のブロックに分割する分割処理と、

前記分割処理で分割されたブロックを離散コサイン変換する離散コサイン変換処理と、

前記離散コサイン変換処理の出力のうちの直流成分を差動符号化する差動符号化処理と、

前記差動符号化処理の出力を量子化する直流量子化処理と、

前記直流量子化処理の出力をエントロピー符号化する直流エントロピー符号化処理と、

前記直流エントロピー符号化処理の出力を暗号化する暗号化処理と、

前記離散コサイン変換処理の出力のうちの交流成分を量子化する交流量子化処理と、

前記交流量子化処理の出力をエントロピー符号化する交流エントロピー符号化処理と、

1画面分の前記暗号化処理の出力ビット数をカウントし、そのカウント値と1画面分の前記暗号化処理の出力と1画面分の前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、

実行すること特徴とする画像データ暗号化方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、デジタル化した画像データを暗号化する画像データ暗号化方法に関するものである。

【0002】

【従来の技術】従来、このような分野の技術としては、例えば次のような文献に記載されるものがあった。

文献1；Communications of the ACM、34[4]（1991-4）（米）Gregory K. Wallace著“ザ ジェビイイーजी スティル ピクチャーコンプレッションスタンダード（The JPEG Still Picture Compression Standard）”P. 30-44

文献2；APPENDIX A.FIPS PUBLICATION46（1977-1）U.S.Department of Commerce/National Bureau of Standards 発行（米）“データエンクリプションスタンダード（Data Encryption Standard）”P. 653-670

文献3；池野・小山著「現代暗号理論」2版（昭62-6-10）電子情報通信学会、P. 43-49

ここで、文献1は画像データの圧縮方法に関する技術であり、文献2、3はデータの暗号化に関する技術である。

【0003】図2は、前記文献1に記載された従来の画像データ圧縮方法の一構成例を示すブロック図である。この画像データ圧縮方法では、例えば縦横8画素のブロック画像データ DA_i がエンコーダ10内の離散コサイン変換部（以下、DCT部という）11で離散コサイン変換（以下、DCT変換という）され、その変換結果が量子化部12へ送られる。量子化部12では、量子化テーブル14のデータに基づいてDCT変換の各係数を量子化し、エントロピー符号化部13へ送る。エントロピー符号化部13は、符号化テーブル15のデータに基づき、量子化部12の出力データに対してエントロピー符号化を行い、圧縮画像データ DA_0 を出力する。これにより、縦横8画素のブロック画像データ DA_i のデータ圧縮が行える。図3は、前記文献2、3に記載された従来のデータ暗号化方法の一構成例を示すブロック図である。このデータ暗号化方法は、暗号化処理部20と鍵の生成部30とでデータの暗号化を行うもので、64ビットからなる平文レジスタ21に入力されたデータは、64ビットからなる鍵レジスタ31に格納したデータに依存して、図3に示される転置、シフト、排他的論理和等の一連の処理によって暗号化され、64ビットからなる暗号文レジスタ23へ出力される。

【0004】暗号化処理部20における暗号化処理では、まず64ビットの平文レジスタ21に対して初期転置IPの処理が行われる。この初期転置IPの処理の出力に対し、16段の暗号化処理22-1～22-16が行われる。初段の暗号化処理22-1では、初期転置IPが行われた64ビットのデータが、32ビットずつ左

右に分割され、左半分が L_0 、及び右半分が R_0 となる。この L_0 と R_0 から L_{16} と R_{16} になるまで、16段にわたって暗号化処理22-1~22-16が行われる。その後、初期転置IPと逆の変換を行う最終転置 IP^{-1} の処理が行われ、暗号化されたデータが64ビットの暗号文レジスタ22に格納される。鍵の生成部30では、第1段~第16段の暗号化処理22-1~22-16に必要な16個の48ビットの鍵 $K_1 \sim K_{16}$ を生成する。まず、パリティビットを含む64ビットの入力鍵が鍵レジスタ31に格納される。鍵レジスタ31の入力鍵に対し、鍵の縮約型転置PC-1により、転置が行われると共にパリティビットが除かれた56ビットの鍵となる。この56ビットの鍵は、2つに分割され、一方の28ビットが C_0 、他方の28ビットが D_0 となる。この C_0 と D_0 をそれぞれ左に順にシフトすることにより、 C_1 、 D_1 から C_{16} 、 D_{16} が順次生成される。n段目の鍵 K_n は、 C_n と D_n からなる56ビットを入力し、鍵の縮約型転置PC-2を行って48ビットとなり、第n段の暗号化処理22-nへ送られる。図4は、図2に示す従来の画像データ圧縮方法と図3に示す従来のデータ暗号化方法とを縦続接続し、画像データ暗号化方法を実現した従来の一構成例を示すブロック図である。この画像データ暗号化方法では、入力端子41から入力された画像データを、図2の画像データ圧縮方法42で圧縮した後、図3のデータ暗号化方法43で暗号化し、その結果を出力端子44から出力する。

【0005】

【発明が解決しようとする課題】しかしながら、上記構成の画像データ暗号化方法では、画像データ圧縮方法42で圧縮された画像データの全てをデータ暗号化方法43で暗号化する必要があるため、暗号化のための処理量が大きくなるという問題がある。これを防止するため、圧縮された画像データの一部を暗号化することも考えられるが、暗号強度が劣化するという欠点があり、未だ技術的十分満足のゆく画像データ暗号化方法を得ることが困難であった。本発明は、前記従来技術が持っていた課題として、暗号強度を犠牲にすることなく、暗号化のための処理量を低減することが困難な点について解決した画像データ暗号化方法を提供するものである。

【0006】

【課題を解決するための手段】第1の発明は、前記課題を解決するために、圧縮した画像データを暗号化する画像データ暗号化方法において、2次元の画像信号をn画素x n画素のブロックに分割する分割処理と、前記分割処理で分割されたブロックをDCT変換するDCT処理と、前記DCT処理の出力のうちの直流成分を量子化する直流量子化処理と、前記DCT処理の出力のうちの交流成分を量子化する交流量子化処理と、前記直流量子化処理の出力を暗号化する暗号化処理とを実行する。さらに、前記交流量子化処理の出力をエントロピー符号化す

る交流エントロピー符号化処理と、前記暗号化処理の出力と前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、実行するようにしている。第2の発明では、第1の発明の画像データ暗号化方法において、前記直流量子化処理では、出力信号をnビットの固定長符号に符号化する固定長符号化処理を行い、前記暗号化処理では、前記直流量子化処理の出力に対してnビット毎に暗号化し、前記多重化処理では、1ブロック毎に前記暗号化処理の出力と前記交流エントロピー符号化処理の出力を多重化するようにしている。第3の発明では、圧縮した画像データを暗号化する画像データ暗号化方法において、2次元の画像信号をn画素x n画素のブロックに分割する分割処理と、前記分割処理で分割されたブロックをDCT変換するDCT処理と、前記DCT処理の出力のうちの直流成分を差動符号化する差動符号化処理と、前記差動符号化処理の出力を量子化する直流量子化処理と、前記直流量子化処理の出力をエントロピー符号化する直流エントロピー符号化処理と、前記直流エントロピー符号化処理の出力を暗号化する暗号化処理とを実行する。さらに、前記DCT処理の出力のうちの交流成分を量子化する交流量子化処理と、前記交流量子化処理の出力をエントロピー符号化する交流エントロピー符号化処理と、1画面分の前記暗号化処理の出力ビット数をカウントし、そのカウント値と1画面分の前記暗号化処理の出力と1画面分の前記交流エントロピー符号化処理の出力とを多重化する多重化処理とを、実行するようにしている。

【0007】

【作用】第1の発明によれば、以上のように画像データ暗号化方法を構成したので、画像信号が入力されると、ブロック処理でブロックに分割され、その分割されたブロックがDCT処理でDCT変換され、直流成分と交流成分が出力される。直流成分は、直流量子化処理で量子化され、暗号化処理で暗号化されて多重化処理へ送られる。DCT処理で出力された交流成分は、交流量子化処理で量子化され、交流エントロピー符号化処理でエントロピー符号化されて多重化処理へ送られる。多重化処理では、暗号化処理の出力と交流エントロピー符号化処理の出力とを多重化する。このように、画像データのうちの直流成分だけを暗号化する。

【0008】一般に、データを圧縮すると、長さが一定でない符号が出力される。圧縮したデータの一部を暗号化する場合、どこからどこまでが暗号化されているのかが、復号化側でわかる必要がある。第1の発明の場合には、多重化後にどこが直流成分で、どこが交流成分かを判別する必要がある。そこで、第2の発明では、直流成分を固定長にすることにより、直流成分と交流成分の判別を行うようにしている。即ち、第2の発明では、DCT処理によって処理された直流成分が、直流量子化処理において該直流成分が量子化され、それが固定長符号

に符号化され、それらの n ビット毎に暗号化処理で暗号化され、多重化処理へ送られる。多重化処理では、1ブロック毎に暗号化処理の出力と交流エントロピー符号化処理の出力を多重化する。このように、直流成分が固定長で符号化されているので、受信側で直流成分の終了の検出が可能となる。

【0009】第3の発明では、直流成分のビット数を付加情報として伝送することにより、前記の直流成分と交流成分の判別を行っている。即ち、この第3の発明では、画像信号が入力されると、分割処理でブロックに分割され、その分割されたブロックがDCT処理でDCT変換され、直流成分と交流成分が出力される。直流成分は、差動符号化処理で差動符号化され、直流エントロピー符号化処理でエントロピー符号化され、暗号化処理で暗号化されて多重化処理へ送られる。DCT処理によって出力された交流成分は、交流量子化処理で量子化され、交流エントロピー符号化処理でエントロピー処理された後、多重化処理へ送られる。多重化処理では、1画面分の暗号化処理の出力ビット数をカウントし、そのカウント値と1画面分の交流エントロピー符号化処理の出力とを多重化する。この多重化された出力の先頭に直流成分のビット長が固定長符号化されているので、受信側で直流成分の終了の検出が可能となる。従って、前記課題を解決できるのである。

【0010】

【実施例】

第1の実施例

図1は、本発明の第1の実施例を示す画像データ暗号化方法の構成ブロック図である。この画像データ暗号化方法では、例えば入力端子101より入力された1画素8ビットからなる信号が、ブロック化部102において縦8画素、横8画素のブロックに分割され、DCT部103へ送られる。DCT部103は、ブロック化部102からのブロックをDCT変換し、直流成分 $f(0, 0)$ のデータ、及び交流成分 $f(i, j)$ のデータを出力する。この直流成分 $f(0, 0)$ は、直流量子化部104において所定のステップサイズQUANT(0, 0)で量子化され、その量子化出力 $q(0, 0)$ が暗号化部110で暗号化された後、該暗号化データが多重化部131へ送られる。DCT部103から出力された交流成分 $f(i, j)$ は、交流量子化部105において所定のステップサイズQUANT(i, j)で量子化され、その

量子化出力 $q(i, j)$ が交流エントロピー符号化部120においてジグザグスキャン等によってエントロピー符号化され、多重化部131へ送られる。多重化部131では、暗号化部110及び交流エントロピー符号化部120の出力を多重化し、固定長で符号化された直流成分DCと可変長符号化された交流成分ACとが、繰り返されて生成された暗号化データが、出力端子132から出力される。この暗号化されたデータは、直流成分DCが固定長で符号化されているので、該データが暗号化されていても、受信側で各成分の終了を検出でき、正しく復号化することが可能となる。

【0011】次に、図1の各ブロックにおける処理内容を図5～図16を参照しつつ説明する。図5は、図1のブロック化部102の処理内容の説明図である。本実施例では、例えば縦288画素、横352画素からなる画像信号を例にとって説明する。図1の入力端子101から入力された縦288画素、横352画素からなる画像信号 $x(i, j)$ は、図1のブロック化部102で、図5に示すように縦36個、横44個のブロックに分割される。

【0012】図6は、ブロック化部102で分割されたブロックのうちの1つのブロック $b(k, l)$ の説明図である。1つのブロック $b(k, l)$ は、図6に示すように、64画素から構成される。 $36 \times 44 = 1584$ 個のブロックは、1個ずつ順に図1のDCT部103へ入力される。入力される順序は任意であるが、本実施例では例えば、 $b(0, 0)$, $b(0, 1)$, $b(0, 2)$, \dots , $b(0, 43)$, $b(1, 0)$, $b(1, 1)$, \dots , $b(35, 42)$, $b(35, 43)$ の順に入力するものとする。図1のDCT部103では、ブロック化部102からのブロックをDCT変換し、直流成分 $f(0, 0)$ のデータ、及び交流成分 $f(i, j)$ のデータを出力する。

【0013】図7は、図1のDCT部103におけるDCT変換の説明図である。例えば、64画素からなる入力データを $e(i, j)$ ($i=0 \sim 7$, $j=0 \sim 7$)とすると図1のDCT部103では次式の演算を行い、出力データ $f(u, v)$ ($u=0 \sim 7$, $v=0 \sim 7$)を出力する。

【0014】

【数1】

$$f(u, v) = \frac{1}{4} C(u) \cdot C(v) \sum_{i=0}^7 \sum_{j=0}^7 e(i, j) \cdot \cos\left(\frac{\pi u(2i+1)}{16}\right) \cdot \cos\left(\frac{\pi v(2j+1)}{16}\right)$$

但し、

$$c(u) = \begin{cases} \frac{1}{\sqrt{2}} & u=0 \\ 1 & u \neq 0 \end{cases}$$

$f(0, 0)$: 直流成分
 $f(0, 0)$ 以外の $f(i, j)$: 交流成分

図1のDCT部103から出力された直流成分 $f(0, 0)$ は、直流量子化部104において次式に従い所定のステップサイズQUANT(0, 0)で量子化され、その量子化出力 $q(0, 0)$ が図1の暗号化部110へ送られる。

$$q(0, 0) = \text{int}[f(0, 0) / \text{QUANT}(0, 0)]$$

ここで、 $\text{int}[\]$ は小数点以下を四捨五入する整数化を表す。例えば、 $f(0, 0)$ は8ビットであるので、QUANT(0, 0) = 8の場合には、量子化出力 $q(0, 0)$ が5ビットとなる。この量子化出力 $q(0, 0)$ は、図1の暗号化部110で暗号化される。

【0015】図8は、図1の暗号化部110の構成ブロック図である。この図では、前記文献2に記載されている64ビット入力、64ビット出力の暗号化方法を5ビットCFB(Cipher Feed Back)モードで用いている。

この暗号化部110は、5ビットの直流成分 $f(0, 0)$ のデータを入力する入力端子111-1~111-5と、初期値を設定する64ビットのシフトレジスタ112とを備え、該シフトレジスタ112の出力側が暗号化部113を介して64ビットのレジスタ114に接続されている。このシフトレジスタ114の出力側と入力端子111-1~111-5は、排他的論理和ゲート115-1~115-6に接続されている。排他的論理和ゲート115-1~115-6の出力側には、パラレル/シリアル変換回路(以下、P/S変換回路という)116と、5ビットの暗号化データを出力する出力端子117-1~117-5とが接続され、該P/S変換回路116の出力側がシフトレジスタ112に接続されてい

る。64ビットのシフトレジスタ112には初期値が設定されており、その初期値が符号化部113で符号化され、その符号化された64ビットのデータがレジスタ114に格納される。入力端子111-1~111-5から入力される5ビットの直流成分 $f(0, 0)$ のデータは、排他的論理和ゲート115-1~115-6において、レジスタ114のうちの例えば左端から5ビットとそれぞれ排他的論理和がとられ、5ビットの暗号化データが出力端子117-1~117-5へ出力される。また、この5ビットの暗号化データは、P/S変換回路116においてシリアルデータに変換され、シフトレジスタ112に入力され、該シフトレジスタ112の内容が5ビット右方向へシフトされる。このシフト結果は、暗号化部113で暗号化され、次のブロックの直流成分 $f(0, 0)$ のデータを暗号化するために用いられる。出力端子117-1~117-5から出力された5ビットの暗号化データは、図1の多重化部131へ送られる。

【0016】一方、図1のDCT部103から出力された交流成分 $f(i, j)$ のデータは、交流量子化部105において次式に従いステップサイズQUANT(i, j)で量子化され、その量子化出力 $q(i, j)$ が交流エントロピー符号化部120へ送られる。

$$q(i, j) = \text{int}[f(i, j) / \text{QUANT}(i, j)]$$

図9は、図1のエントロピー符号化部120の構成ブロック図である。この交流エントロピー符号化部120は、交流量子化部105からの量子化出力 $q(i, j)$ を入力する入力端子121を有し、それにはジグザグスキャン部122を介してゼロ判定部123が接続されて

いる。ゼロ判定部123の出力側には、ランレンゲスカウント部124及びグループ化部125が接続され、そのランレンゲスカウント部124及びグループ化部125の出力側に、2次元ハフマン符号化部126が接続されている。さらに、2次元ハフマン符号化部126の出力側とグループ化部125の出力側には、多重化部127が接続され、さらにその出力側に出力端子128が接続されている。入力端子121より入力された交流成分の量子化出力 $q(i, j)$ は、ジグザグスキャン部122に入力される。図10は、図9のジグザグスキャン部122の説明図である。ジグザグスキャン部122では、図10に示すように、矢印の方向に交流成分 $f(i, j)$ のデータをスキャンし、2次元の $f(i, j)$ を1次元に並び換える。このジグザグスキャン部122の出力は、例えば、 $f(0, 1)$, $f(1, 0)$, $f(2, 0)$, $f(1, 1)$, $f(0, 2)$, $f(0, 3)$, \dots , $f(7, 7)$ のような順序になり、図9のゼロ判定部123へ入力される。

【0017】ゼロ判定部123では、入力された交流成分 $f(i, j)$ のデータがゼロであるかどうかを判定する。ゼロである場合には、ランレンゲスカウント部124においてカウンタの値が+1増分され、そのゼロの連続の数(ラン)Nが2次元ハフマン符号化部126へ送られる。ゼロ判定部123においてゼロでないと判定された場合には、交流成分 $f(i, j)$ のデータがグループ化部125においてグループ番号Sと付加ビットDが求められ、そのグループ番号Sが2次元ハフマン符号化部126へ送られると共に、該付加ビットDが多重化部127へ送られる。図11は、交流成分 $f(i, j)$ とグループ番号S及び付加ビットDの関係を示す図である。例えば、入力された交流成分 $f(i, j) = -2$ の場合には、グループ番号 $S = 2$ 、付加ビット $D = 10$ となる。グループ化部125よりグループ番号Sが2次元ハフマン符号化部126へ送られると、該2次元ハフマン符号化部126には、ランレンゲスカウント部124より現在までのランNが入力される。ランレンゲスカウント部124の内部のカウンタは、次のゼロランの数をカウントするために、ゼロにリセットされる。図12、図13、及び図14は、2次元ハフマン符号化部126で用いられるハフマン符号化テーブルの例を示す図である。2次元ハフマン符号化部126では、図12～図14に示すハフマン符号化テーブルに基づき、ランNとグループ番号Sからハフマン符号化を行い、符号化されたコードCを多重化部127へ出力する。例えば、ラン $N = 5$ 、グループ番号 $S = 2$ の場合には、2次元ハフマン符号化部126からコード $C = 11111110111$ が出力され、多重化部127へ送られる。多重化部127では、2次元ハフマン符号化部126からのコードCとグループ化部125からの付加ビットDとを直列に並べて多重化し、その出力データを出力端子128から出

力して図1の多重化部131へ送る。これら一連の動作が、 $f(7, 7)$ までの全ての交流成分がジグザグスキャン部122より入力されるまで繰り返される。例えば、図1の交流量子化部105からの入力系列が1, 0, 0, 0, 0, 0, -2, \dots であるとき、図1の多重化部131への出力は、00011111111011110 \dots となる。図15は、この例の場合の交流エントロピー符号化部120の動作説明図である。

【0018】図1の交流エントロピー符号化部120では、図15に示すように、最初の1が図9のジグザグスキャン部122から入力されると、それまでのゼロランの数 $N = 0$ 、図11より1のグループ番号 $S = 1$ であるので、図12～図14より、コード $C = 00$ が図9の多重化部127へ出力される。引き続き、図11より、1の付加コード $D = 0$ が図9の多重化部127へ出力される。次に、5個の0に引き続いて-2が入力されるので、 $N = 5$ 、 $S = 2$ で $C = 11111110111$ 、 $D = 10$ が図9の多重化部127へ出力される。このような図1の交流エントロピー符号化部120の出力が多重化部131に入力され、該多重化部131において暗号化部110の出力とブロック毎に多重化され、出力端子132から出力される。図16に、出力端子132からの出力信号のフォーマットを示す。このフォーマットでは、5ビットの固定長で符号化された直流成分DCと、可変長符号化された交流成分ACが、1584ブロック繰り返される。このように、直流成分DCが固定長で符号化されているので、入力画像データが符号化されていても、受信側で各成分の終了を検出でき、正しく復号化することが可能となる。以上のように、本実施例では、直流成分 $f(0, 0)$ だけを暗号化部110で暗号化するようにしたので、暗号強度を犠牲にすることなく、暗号化のための処理量を低減できる。例えば、352画素 \times 288画素からなる約2.5Mbitの画像データを扱う場合、従来の図4の画像データ暗号化方法では、約70Kbitのデータを暗号化しなければならないのに対し、本実施例を用いると、約6Kbitのデータを暗号化するだけでよい。そのため、暗号化のための処理量が約1/10に低減できる。

【0019】第2の実施例

図17は、本発明の第2の実施例を示す画像データ暗号化方法の構成ブロック図であり、第1の実施例を示す図1中の要素と共通の要素には共通の符号が付されている。この画像データ暗号化方法では、図1のDCT部103の出力側と直流量子化部104の入力側との間に、直流成分 $f(0, 0)$ を差動符号化する差動符号化部140が接続されている。さらに、図1の直流量子化部104の出力側に、エントロピー符号化を行って可変長符号化を施す直流エントロピー符号化部150と、該直流エントロピー符号化部150の出力を暗号化する暗号化

部160とを介して、多重化部170が接続されている。多重化部170は、暗号化部160の出力と交流エントロピー符号化部120の出力とを多重化し、それを出力端子132から出力する機能を有している。この画像データ符号化方法では、画像信号が入力端子101から入力されると、それがブロック化部102でブロックに分割され、分割されたブロックがDCT部103でDCT変換され、直流成分 $f(0, 0)$ のデータ及び交流成分 $f(i, j)$ のデータが出力される。DCT部103から出力された直流成分 $f(0, 0)$ のデータは、差動符号化部140において前ブロックの直流成分との差が求められ、その差が直流量子化部104で量子化され、直流エントロピー符号化部150でエントロピー符号化された後、暗号化部160で暗号化されて多重化部170へ送られる。

【0020】一方、DCT部103から出力された交流成分 $f(i, j)$ のデータは、第1の実施例と同様に、交流量子化部105で量子化され、交流エントロピー符号化部120でエントロピー符号化された後、多重化部170へ送られる。多重化部170では、暗号化部160の出力と交流エントロピー符号化部120の出力とを多重化し、出力端子132から出力する。次に、図17の各ブロックの処理を、図18～図21を参照しつつ説明する。図18は、図17の直流エントロピー符号化部150の内部構成を示すブロック図である。この直流エントロピー符号化部150は、図17の直流量子化部104の出力を入力する入力端子151を有し、それにはグループ化部152が接続されている。グループ化部152は、入力端子151の入力をグループ化し、グループ番号S及び付加ビットDを出力する機能を有し、該グループ番号Sが1次元ハフマン符号化部153へ、該付加ビットDが多重化部154へ送られる。1次元ハフマン符号化部153は、グループ番号Sに基づきハフマン符号化を行い、コードCを多重化部154へ出力する機能を有している。多重化部154は、コードCと付加ビットDを多重化して出力端子155へ出力する機能を有している。図18の直流エントロピー符号化部150において、図17の直流量子化部104の出力が入力端子151より入力され、その入力データがグループ化部152においてグループ化され、グループ番号Sが1次元ハフマン符号化部153へ、付加ビットDが多重化部154へ送られる。グループ化部152では、例えば図11と同一のデータに基づき、グループ化処理を行う。1次元ハフマン符号化部153は、例えば図19に示すハフマン符号化テーブルを用い、入力されたグループ番号Sをハフマン符号化により可変長符号化し、コードCを多重化部154へ出力する。例えば、グループ番号S=5のときには、図19に示すように、コードC=110が出力される。多重化部154は、コードCと付加ビットDを多重化し、その直列データを出力端子155を介

して図17の暗号化部160へ出力する。

【0021】図17の暗号化部160では、例えば前記文献2に記載された方法により、直流エントロピー符号化部150より入力されるデータを64ビット毎にブロック化して暗号化し、多重化部170へ送る。なお、第1の実施例を示す図1の暗号化部110と同様に、CFBモードを用いて暗号化することも可能である。DCT部103から出力された交流成分 $f(i, j)$ のデータは、第1の実施例と同様に、交流量子化部105で量子化され、交流エントロピー符号化部120でエントロピー符号化された後、多重化部170へ送られる。図20は、図17の多重化部170の内部構成を示すブロック図である。この多重化部170は、図17の暗号化部160の出力を入力する入力端子171と、交流エントロピー符号化部120の出力を入力する入力端子172とを備え、それらの入力端子171, 172にデータ一時格納用のバッファ173, 174が接続されている。バッファ173の出力側には、ビット数カウント部175及び多重化部176が接続され、さらにバッファ174の出力側が該多重化部176に接続され、該多重化部176の出力側に出力端子132が接続されている。この多重化部170では、入力端子171, 172より入力された図17の暗号化部160及び交流エントロピー符号化部120の出力データが、バッファ173, 174に1画面1584ブロック分が蓄積される。1画面分がバッファ173, 174にそれぞれ蓄積されると、該バッファ173に蓄積された直流成分の暗号化されたデータが、ビット数カウント部175へ送られる。ビット数カウント部175は、バッファ173に蓄積されたビット数をカウントし、多重化部176へ送る。多重化部176は、バッファ173の出力データとバッファ174の出力データを多重化し、出力端子132へ出力する。図21は、図17及び図20の出力端子132から出力される出力信号のフォーマットである。先頭に直流成分DCのビット長を固定長符号化しているので、受信側で直流成分DCの終了を検出でき、正しく復号できる。

【0022】以上のように、本実施例では、DCT部103から出力された直流成分 $f(0, 0)$ に対し、差動符号化部140で差動符号化を行い、直流エントロピー符号化部150でエントロピー符号化を行い、可変長符号化を施している。この場合、直流成分 $f(0, 0)$ が暗号化部160で暗号化されても、受信側で直流成分DCの終わりが検出できるように、例えば1584ブロック全体の直流成分DCを多重化部170内のバッファ173, 174に蓄えて該直流成分DCの長さをビット数カウント部175でカウントし、その長さを出力端子132からの出力系列の先頭に固定長符号で付加している。そのため、受信側で直流成分の終了を検出でき、正しく復号できるので、第1の実施例と同様に、暗号強度を犠牲にすることなく、暗号化のための処理量を低減で

きる。

【0023】なお、本発明は上記実施例に限定されず、例えば、図1の暗号化部110、及び交流エントロピー符号化部120を、図8及び図9以外の構成で処理することも可能である。同様に、図17の直流エントロピー符号化部150、及び多重化部170を、図18及び図20以外の構成で処理することも可能である。

【0024】

【発明の効果】以上詳細に説明したように、第1の発明によれば、画像データの最も重要な情報を含む直流成分だけを暗号化するようにしたので、暗号強度を犠牲にすることなく、暗号化のための処理量を低減することができる。第2の発明によれば、直流成分が固定長で符号化されるので、入力画像信号が暗号化されていても、受信側で直流成分と交流成分の終了を検出でき、正しく復号化することが可能となる。特に、受信ブロック毎に復号を開始できる効果がある。第3の発明によれば、直交変換された直流成分に差動符号化やエントロピー符号化を用いて可変長符号化を施している。この際、多重化処理において暗号化処理の出力ビット数をカウントし、その

【図面の簡単な説明】

【図1】本発明の第1の実施例を示す画像データ暗号化方法の構成ブロック図である。

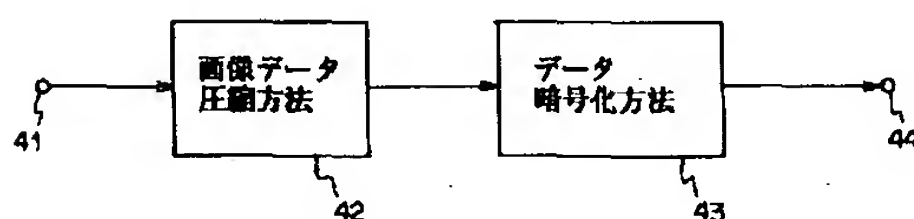
【図2】従来の画像データ圧縮方法の構成ブロック図である。

【図3】従来のデータ暗号化方法の構成ブロック図である。

【図4】従来の画像データ暗号化方法の構成ブロック図である。

【図5】図1のブロック化部の説明図である。

【図4】



従来の画像データ暗号化方法

【図6】図1のブロック化データの説明図である。

【図7】図1のDCT変換の説明図である。

【図8】図1の暗号化部の構成ブロック図である。

【図9】図1の交流エントロピー符号化部の構成ブロック図である。

【図10】図9のジグザグスキャン部の説明図である。

【図11】図9の交流成分 $f(i, j)$ とグループ番号 S 及び付加ビット D の関係を示す図である。

【図12】図9の2次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

【図13】図9の2次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

【図14】図9の2次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

【図15】図1のエントロピー符号化部の説明図である。

【図16】図1の多重化部における出力信号のフォーマットを示す図である。

【図17】本発明の第2の実施例を示す画像データ暗号化方法の構成ブロック図である。

【図18】図17の直流エントロピー符号化部の構成ブロック図である。

【図19】図18の1次元ハフマン符号化部で用いるハフマン符号化テーブルを示す図である。

【図20】図17の多重化部の構成ブロック図である。

【図21】図17の多重化部における出力信号のフォーマットを示す図である。

【符号の説明】

102	ブロック化部
103	DCT部
104	直流量子化部
105	交流量子化部
110, 160	暗号化部
120	交流エントロピー符号化部
131, 170	多重化部
140	差動符号化部
150	直流エントロピー符号化部

【図15】

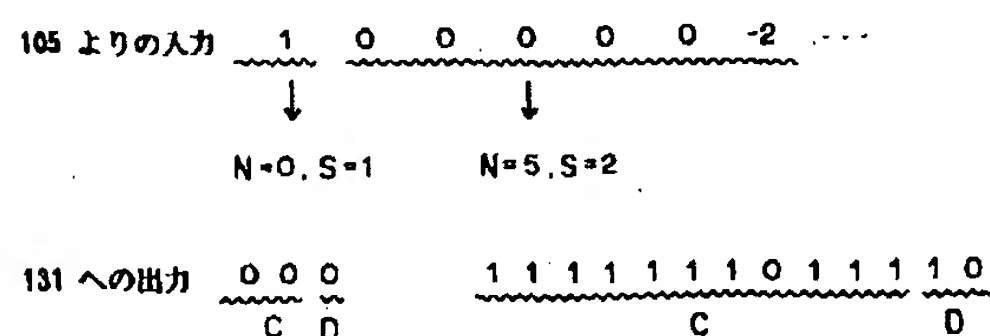
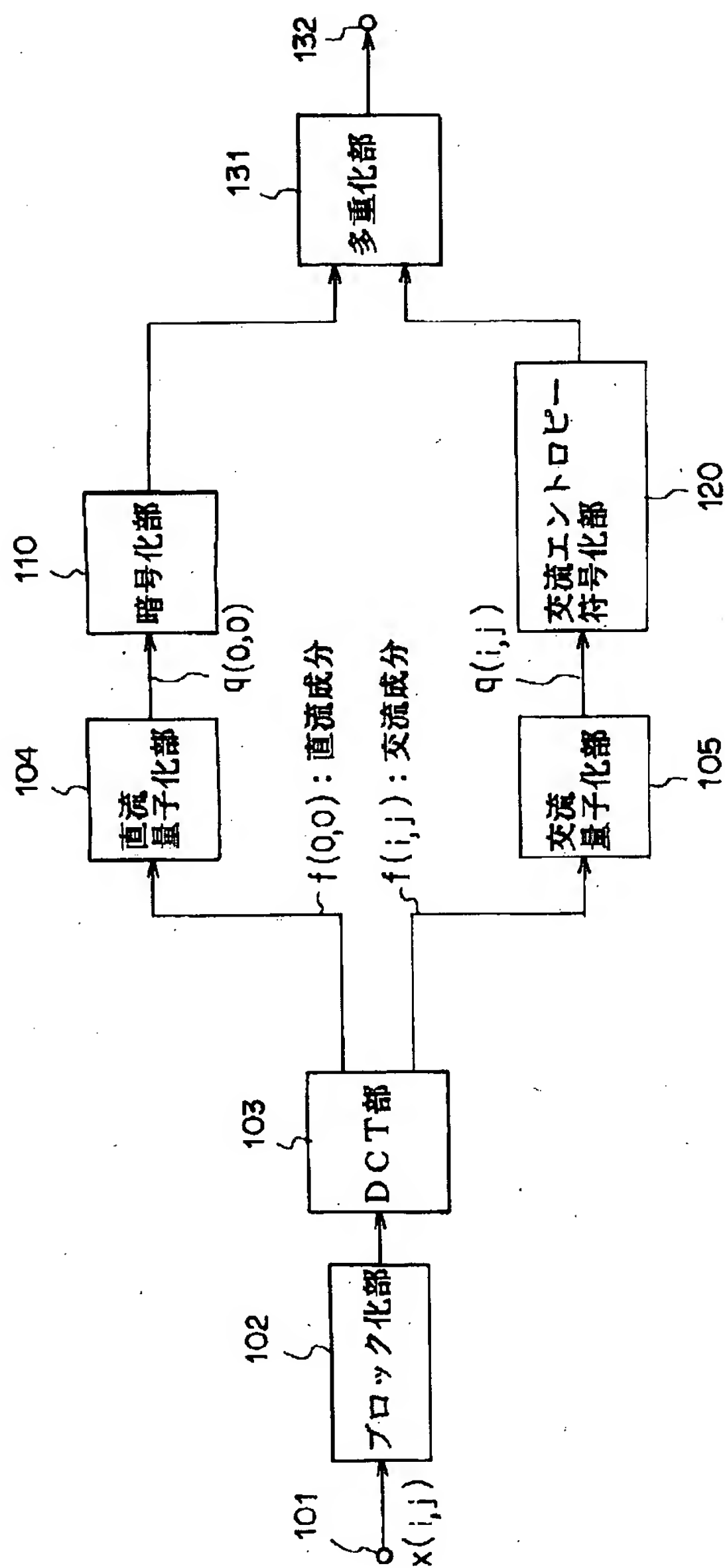


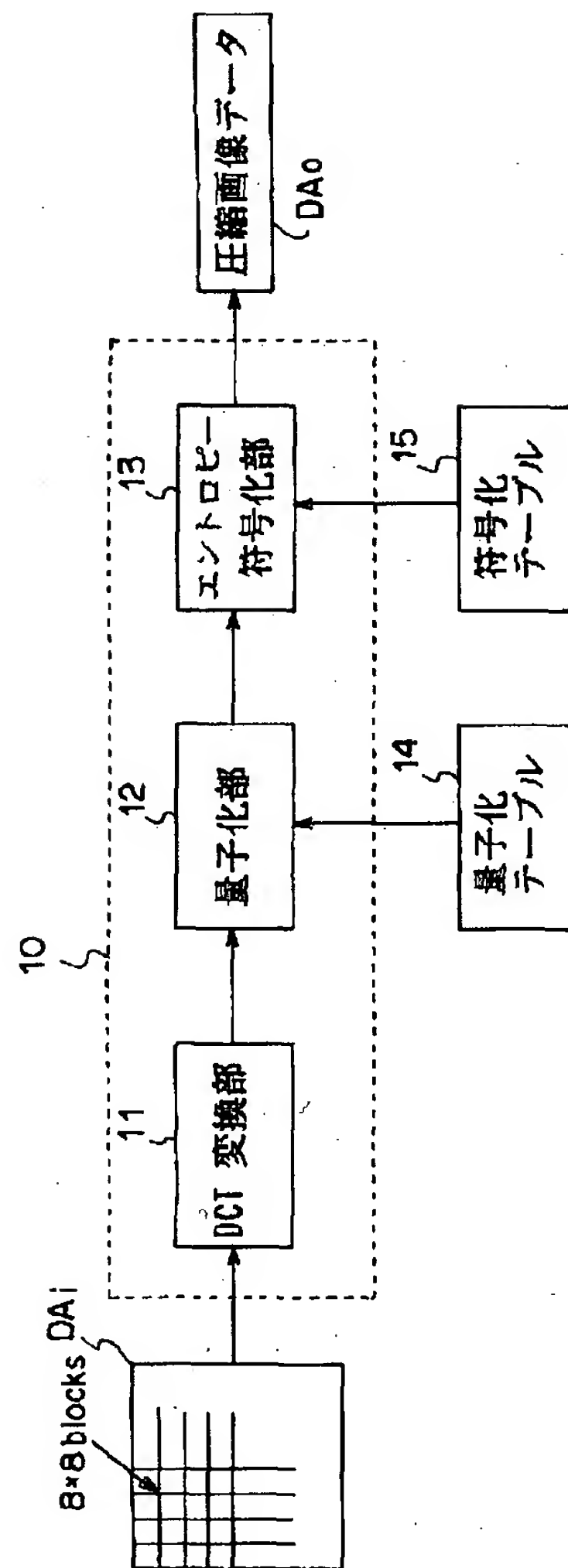
図1のエントロピー符号化部

【図1】



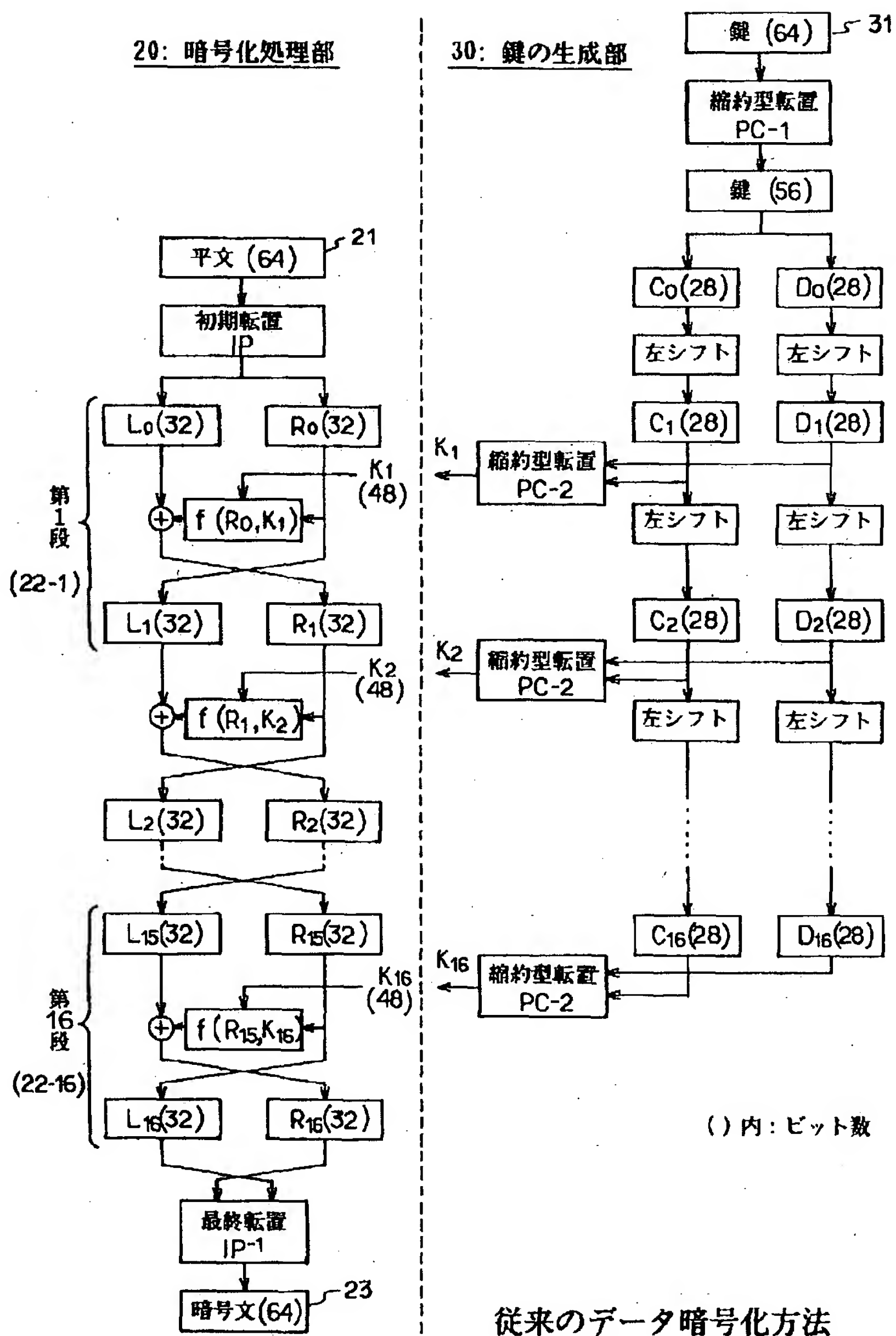
本発明の第1の実施例の画像データ暗号化方法

【図2】



従来の画像データ圧縮方法

【図3】



【図5】

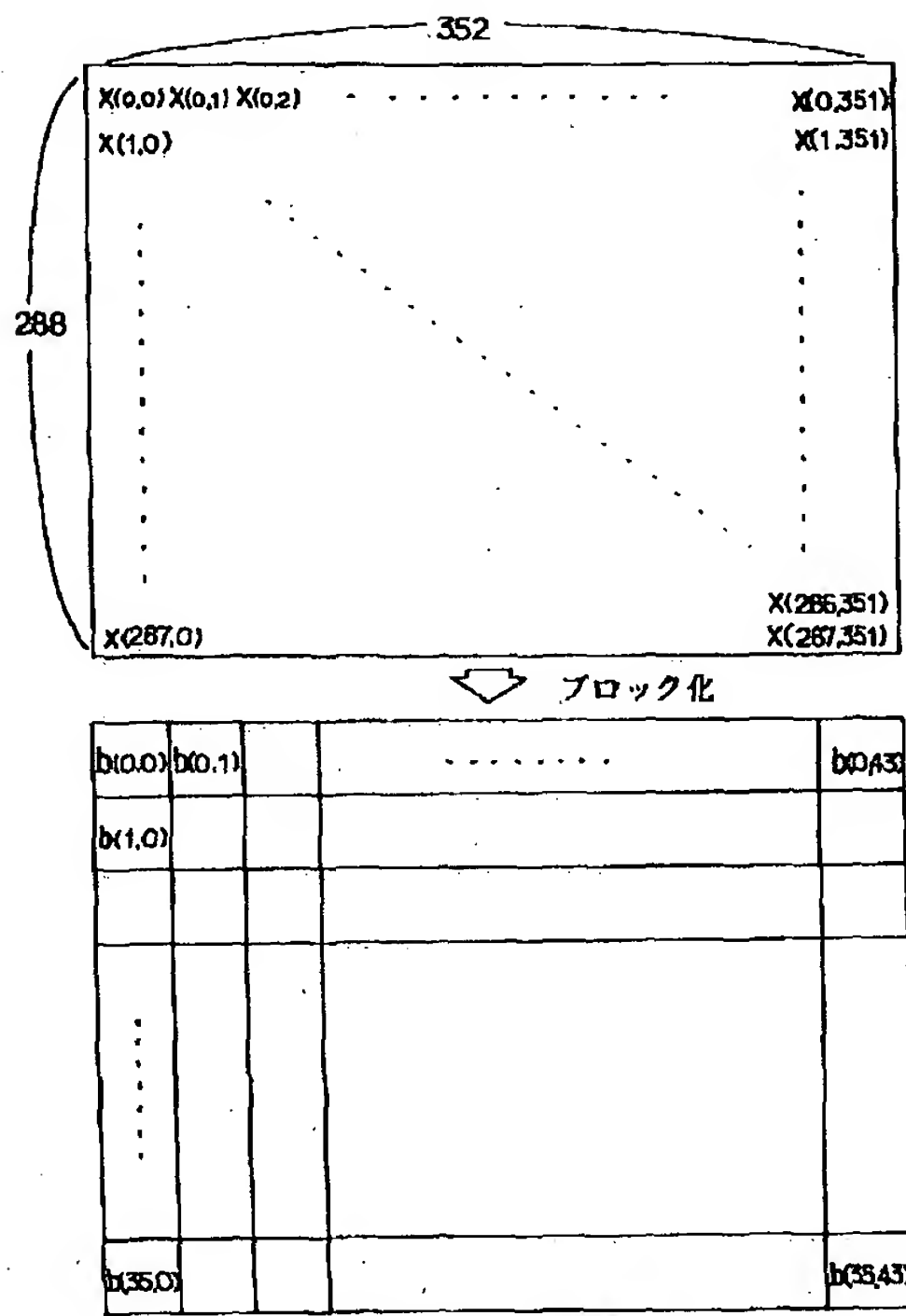


図1のブロック化部

【図6】

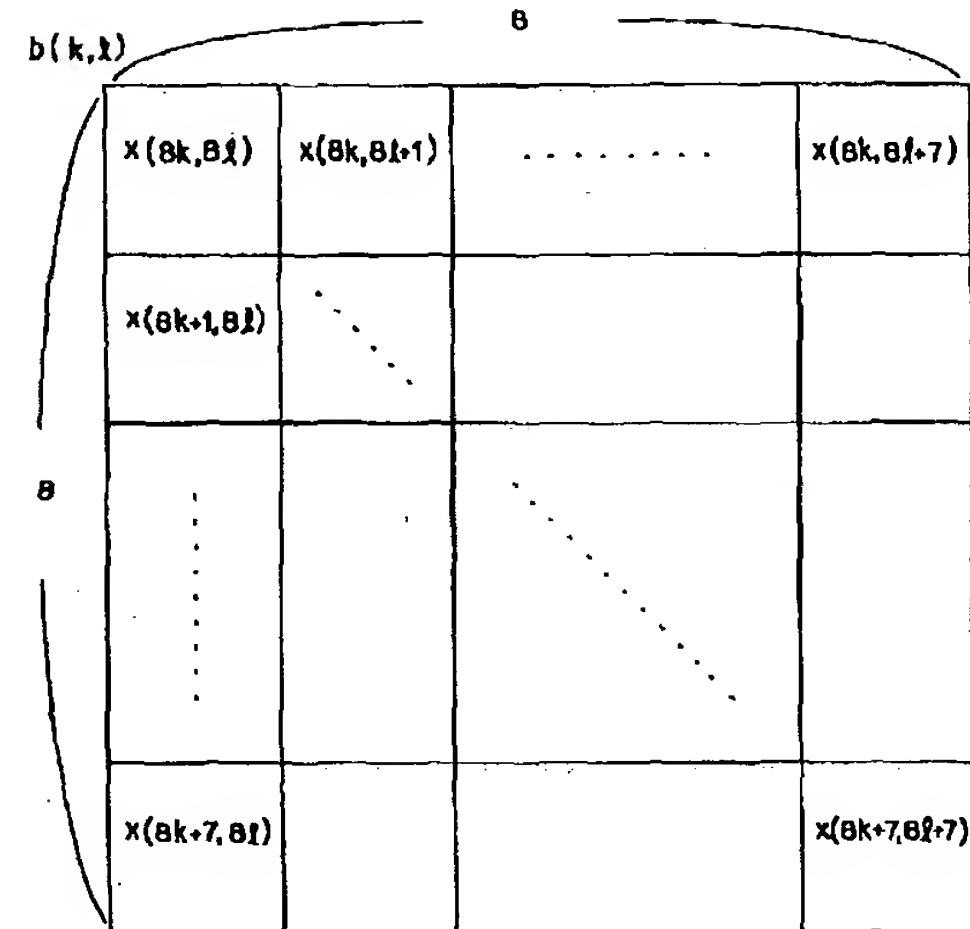


図1のブロック化データ

【図8】

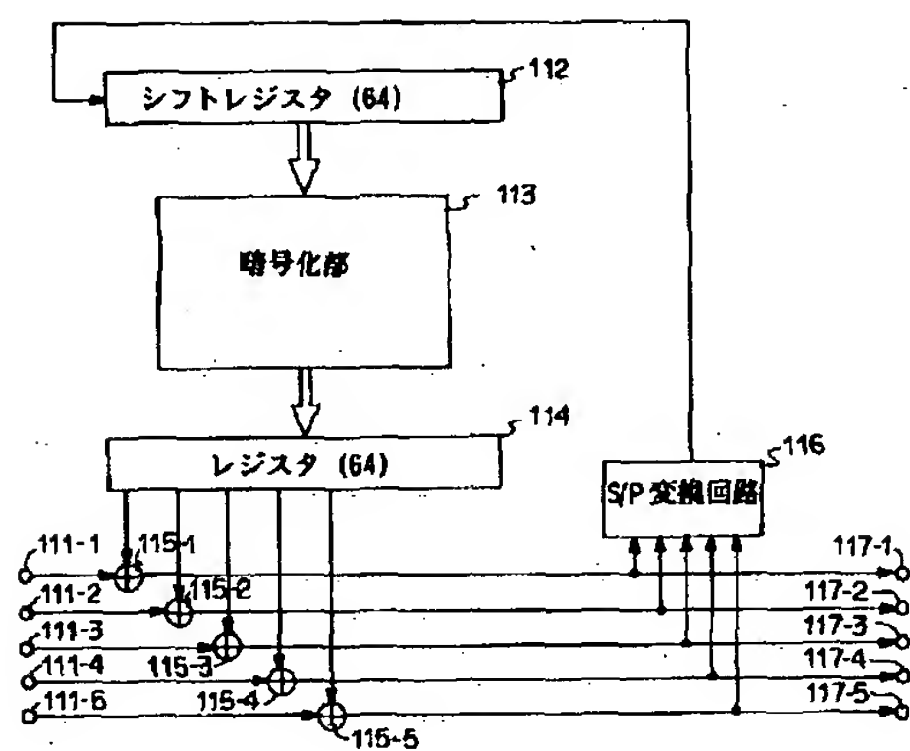


図1の暗号化部

【図10】

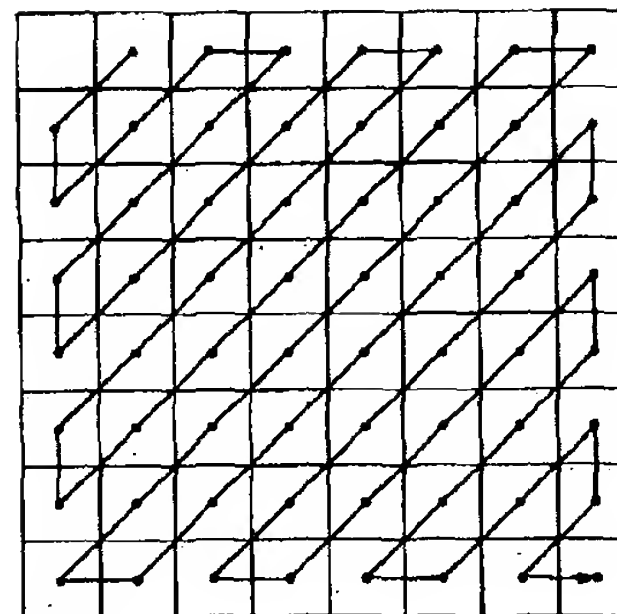


図9のジグザグスキャン部

【図7】

DCT
↑

$e(0,0)$	$e(0,1)$	$e(0,2)$	$e(0,3)$	$e(0,4)$	$e(0,5)$	$e(0,6)$	$e(0,7)$	$f(0,0)$	$f(0,1)$	$f(0,2)$	$f(0,3)$	$f(0,4)$	$f(0,5)$	$f(0,6)$	$f(0,7)$
$e(1,0)$	$e(1,1)$	$e(1,2)$	$e(1,3)$	$e(1,4)$	$e(1,5)$	$e(1,6)$	$e(1,7)$		$f(1,1)$	$f(1,2)$	$f(1,3)$	$f(1,4)$	$f(1,5)$	$f(1,6)$	$f(1,7)$
$e(2,0)$	$e(2,1)$	$e(2,2)$	$e(2,3)$	$e(2,4)$	$e(2,5)$	$e(2,6)$	$e(2,7)$		$f(2,1)$	$f(2,2)$	$f(2,3)$	$f(2,4)$	$f(2,5)$	$f(2,6)$	$f(2,7)$
$e(3,0)$	$e(3,1)$	$e(3,2)$	$e(3,3)$	$e(3,4)$	$e(3,5)$	$e(3,6)$	$e(3,7)$		$f(3,1)$	$f(3,2)$	$f(3,3)$	$f(3,4)$	$f(3,5)$	$f(3,6)$	$f(3,7)$
$e(4,0)$	$e(4,1)$	$e(4,2)$	$e(4,3)$	$e(4,4)$	$e(4,5)$	$e(4,6)$	$e(4,7)$		$f(4,1)$	$f(4,2)$	$f(4,3)$	$f(4,4)$	$f(4,5)$	$f(4,6)$	$f(4,7)$
$e(5,0)$	$e(5,1)$	$e(5,2)$	$e(5,3)$	$e(5,4)$	$e(5,5)$	$e(5,6)$	$e(5,7)$		$f(5,1)$	$f(5,2)$	$f(5,3)$	$f(5,4)$	$f(5,5)$	$f(5,6)$	$f(5,7)$
$e(6,0)$	$e(6,1)$	$e(6,2)$	$e(6,3)$	$e(6,4)$	$e(6,5)$	$e(6,6)$	$e(6,7)$		$f(6,1)$	$f(6,2)$	$f(6,3)$	$f(6,4)$	$f(6,5)$	$f(6,6)$	$f(6,7)$
$e(7,0)$	$e(7,1)$	$e(7,2)$	$e(7,3)$	$e(7,4)$	$e(7,5)$	$e(7,6)$	$e(7,7)$		$f(7,1)$	$f(7,2)$	$f(7,3)$	$f(7,4)$	$f(7,5)$	$f(7,6)$	$f(7,7)$

図1のDCT変換

【図9】

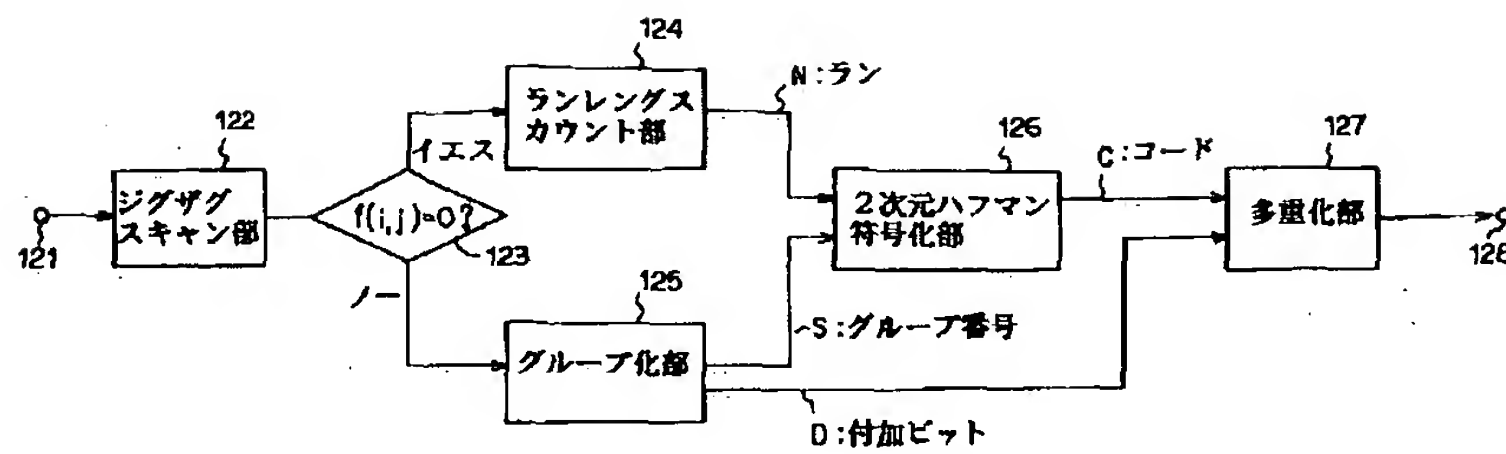


図1の交流エントロピー符号化部

【図11】

$f(i, j)$	グループ番号 S	付加ビット D
-32767	15	1111111111111111
-32766		1111111111111110
⋮		⋮
-16384		1000000000000000
-16383	14	1111111111111111
⋮		⋮
⋮		⋮
⋮		1000000000000000
⋮	⋮	⋮
-3	2	11
-2	2	10
-1	1	1
0	0	なし
1	1	0
⋮	⋮	⋮
16384	15	0000000000000000
⋮		⋮
32767		0111111111111111
32768		なし

交流成分 $f(i, j)$ とグループ番号 S 及び付加ビット D の関係

【図12】

N/S	符号長	C
0/0 (EOB)	4	1010
0/1	2	00
0/2	2	01
0/3	3	100
0/4	4	1011
0/5	5	11010
0/6	7	1111000
0/7	8	11111000
0/8	10	1111110110
0/9	16	111111110000010
0/A	16	111111110000011
1/1	4	1100
1/2	5	11011
1/3	7	1111001
1/4	9	111110110
1/5	11	11111110110
1/6	16	111111110000100
1/7	16	111111110000101
1/8	16	111111110000110
1/9	16	111111110000111
1/A	16	111111110001000
2/1	5	11100
2/2	8	11111001
2/3	10	1111110111
2/4	12	111111110100
2/5	16	111111110001001
2/6	16	111111110001010
2/7	16	111111110001011
2/8	16	111111110001100
2/9	16	111111110001101
2/A	16	111111110001110
3/1	6	111010
3/2	9	111110111
3/3	12	111111110101
3/4	16	111111110001111
3/5	16	111111110010000
3/6	16	111111110010001
3/7	16	111111110010010
3/8	16	111111110010011
3/9	16	111111110010100
3/A	16	111111110010101
4/1	6	111011
4/2	10	1111111000
4/3	16	111111110010110
4/4	16	111111110010111
4/5	16	111111110011000
4/6	16	111111110011001
4/7	16	111111110011010
4/8	16	111111110011011
4/9	16	111111110011100
4/A	16	111111110011101
5/1	7	1111010
5/2	11	11111110111
5/3	16	111111110011110

ハフマン符号化テーブル

【図13】

N/S	符号長	C
5/4	16	1111111110011111
5/5	16	1111111110100000
5/6	16	1111111110100001
5/7	16	1111111110100010
5/8	16	1111111110100011
5/9	16	1111111110100100
6/A	16	1111111110100101
6/1	7	1111011
6/2	12	111111110110
6/3	16	1111111110100110
6/4	16	1111111110100111
6/5	16	1111111110101000
6/6	16	1111111110101001
6/7	16	1111111110101010
6/8	16	1111111110101011
6/9	16	1111111110101100
6/A	16	1111111110101101
7/1	8	11111010
7/2	12	111111110111
7/3	16	1111111110101110
7/4	16	1111111110101111
7/5	16	1111111110110000
7/6	16	1111111110110001
7/7	16	1111111110110010
7/8	16	1111111110110011
7/9	16	1111111110110100
7/A	16	1111111110110101
8/1	9	111111000
8/2	15	1111111110000000
8/3	16	1111111110110110
8/4	16	1111111110110111
8/5	16	1111111110111000
8/6	16	1111111110111001
8/7	16	1111111110111010
8/8	16	1111111110111011
8/9	16	1111111110111100
8/A	16	1111111110111101
9/1	9	111111001
9/2	16	1111111110111110
9/3	16	1111111110111111
9/4	16	1111111111000000
9/5	16	1111111111000001
9/6	16	1111111111000010
9/7	16	1111111111000011
9/8	16	1111111111000100
9/9	16	1111111111000101
9/A	16	1111111111000110
A/1	9	111111010
A/2	16	1111111111000111
A/3	16	1111111111001000
A/4	16	1111111111001001
A/5	16	1111111111001010
A/6	16	1111111111001011
A/7	16	1111111111001100

ハフマン符号化テーブル

【図14】

N/S	符号長	C
A/8	16	1111111111001101
A/9	16	1111111111001110
A/A	16	1111111111001111
B/1	10	1111111001
B/2	16	1111111111010000
B/3	16	1111111111010001
B/4	16	1111111111010010
B/5	16	1111111111010011
B/6	16	1111111111010100
B/7	16	1111111111010101
B/8	16	1111111111010110
B/9	16	1111111111010111
B/A	16	1111111111011000
C/1	10	1111111010
C/2	16	1111111111011001
C/3	16	1111111111011010
C/4	16	1111111111011011
C/5	16	1111111111011100
C/6	16	1111111111011101
C/7	16	1111111111011110
C/8	16	1111111111011111
C/9	16	1111111111100000
C/A	16	1111111111100001
D/1	11	11111111000
D/2	16	1111111111100010
D/3	16	1111111111100011
D/4	16	1111111111100100
D/5	16	1111111111100101
D/6	16	1111111111100110
D/7	16	1111111111100111
D/8	16	1111111111101000
D/9	16	1111111111101001
D/A	16	1111111111101010
E/1	16	1111111111101011
E/2	16	1111111111101100
E/3	16	1111111111101101
E/4	16	1111111111101110
E/5	16	1111111111101111
E/6	16	1111111111110000
E/7	16	1111111111110001
E/8	16	1111111111110010
E/9	16	1111111111110011
E/A	16	1111111111110100
F/0(ZRL)	11	11111111001
F/1	16	1111111111110101
F/2	16	1111111111110110
F/3	16	1111111111110111
F/4	16	1111111111111000
F/5	16	1111111111111001
F/6	16	1111111111111010
F/7	16	1111111111111011
F/8	16	1111111111111100
F/9	16	1111111111111101
F/A	16	1111111111111110

ハフマン符号化テーブル

【図16】

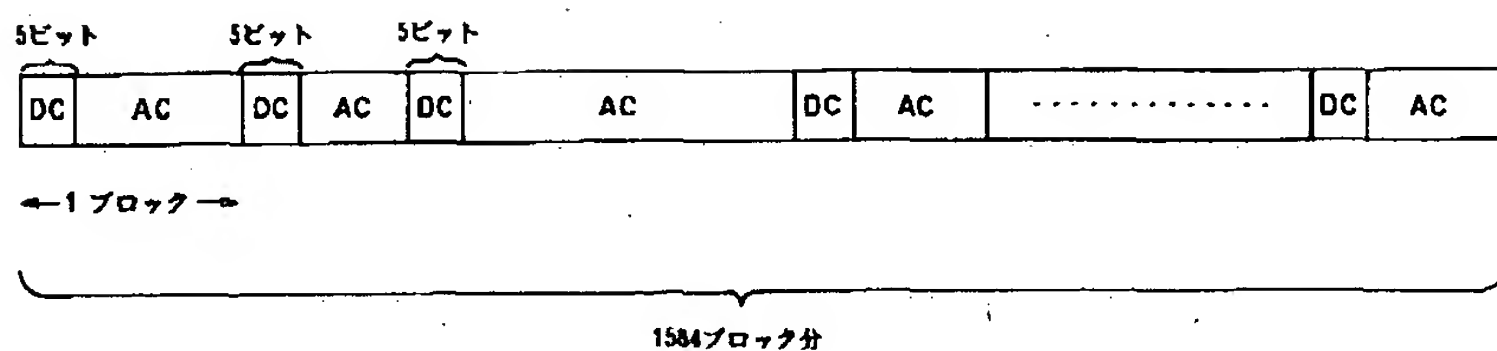
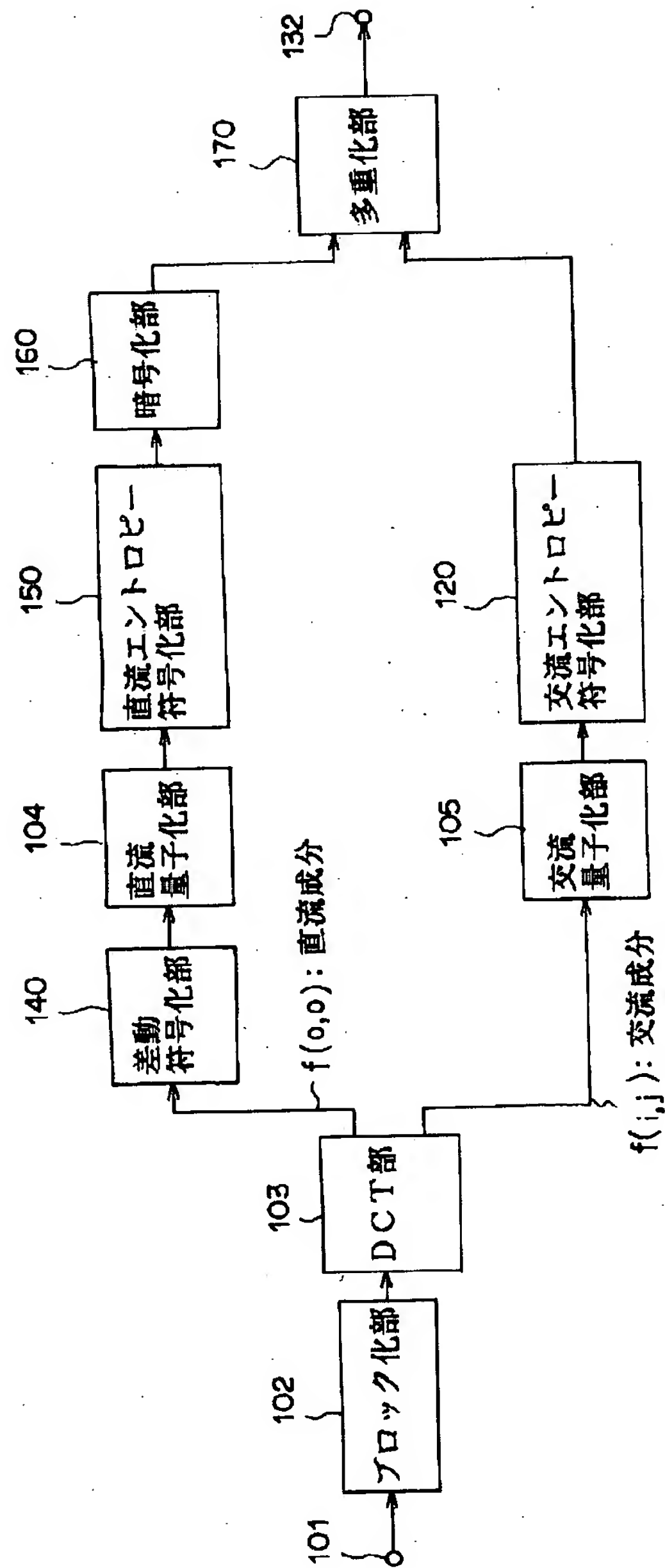


図1の多重化部の出力信号のフォーマット

【図17】



本発明の第2の実施例の画像データ暗号化方法

【図18】

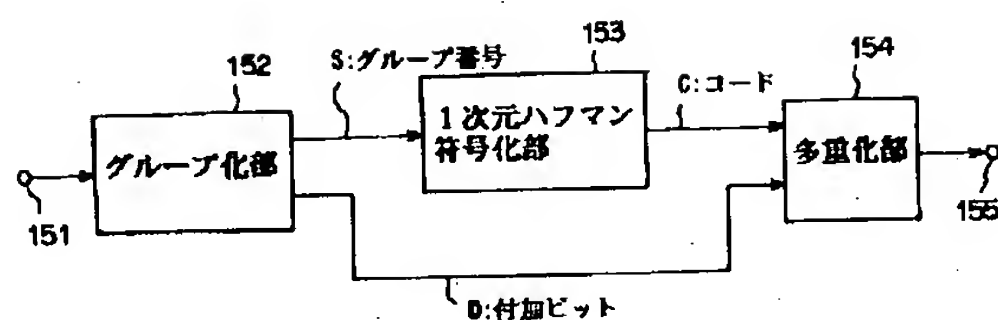


図17の直流エントロピー符号化部

【図19】

S	C
0	0 0
1	0 1 0
2	0 1 1
3	1 0 0
4	1 0 1
5	1 1 0
6	1 1 1 0
7	1 1 1 1 0
8	1 1 1 1 1 0
9	1 1 1 1 1 1 0
10	1 1 1 1 1 1 1 0
11	1 1 1 1 1 1 1 1 0

ハフマン符号化テーブル

【図20】

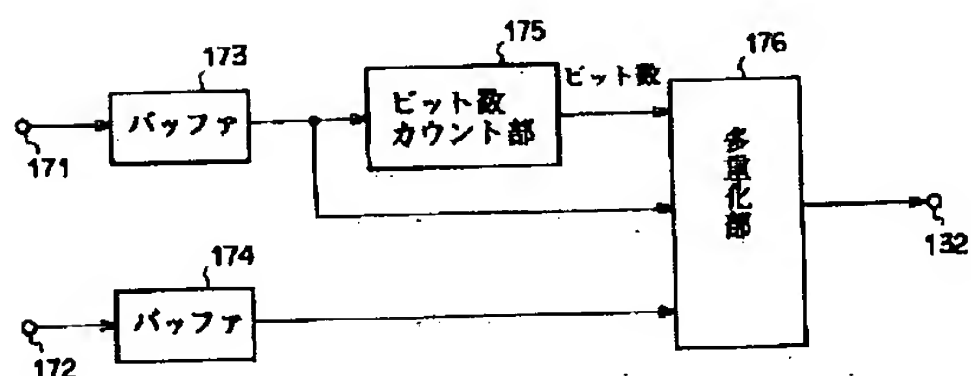


図17の多重化部

【図21】

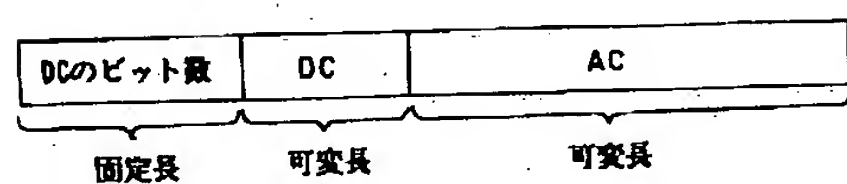


図17の多重化部の出力信号のフォーマット

フロントページの続き

(51) Int. Cl. 5

H 0 4 L 9/14

H 0 4 N 1/41

1/415

1/44

7/133

識別記号

庁内整理番号

F I

技術表示箇所

B 9070-5C

9070-5C

2109-5C

Z